(U//FOUO) CCIC Alert - Data Breach Incident at Law Enforcement Website Provider

info@sacrtac.org

Wed 6/24/2020 2:58 PM

To:info@sacrtac.org <info@sacrtac.org>;

UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U//FOUO) Central California Intelligence Center (CCIC) Alert: Data Breach Incident at Law Enforcement Website Provider.

(U//FOUO) You may receive more than one copy of this message as the CCIC reaches out to all partners.

(U//FOUO) On 19 June 2020, the National Fusion Center Association (NFCA) alerted the CCIC to a data breach targeting Netsential[USBUS], a web development firm used by fusion centers, including the CCIC, and law enforcement agencies nationwide. The FBI reports at least 296 GB of data were exfiltrated.

(U//FOUO) **You are receiving this email because you may be impacted by this data breach. Data exposed may include information you provided while signing up for TLO training and access, such as agency affiliation and contact information. This data leak was posted on an untrusted dark web forum; partners are discouraged from independently downloading or investigating the data.**

(U//FOUO) The CCIC is working with local, State, and Federal partners to mitigate the impact of the breach, and will continue to provide updates, as needed.

(U//FOUO) The CCIC is asking its partners to maintain operational and situational awareness, and monitor for phishing and vishing (voice phishing) attacks.

(U//FOUO) If you have an active user account with access to our website, we recommend you immediately initiate a password reset by clicking the following link: reset password. Netsential has added a multifactor user authentication to increase security.

(U//FOUO) The CCIC also recommends the following cyber hygiene actions:

- (U//FOUO) Change passwords, incorporating special characters, and upper and lower case letters.
- (U//FOUO) Update antivirus software, install patches, implement multi-factor authentication, and disable attachment macros.
- (U//FOUO) Be vigilant of links and attachments in emails, especially with attention-grabbing subject lines, and from unexpected or unknown senders. Carefully examine senders' email addresses for any inconsistencies.
- (U//FOUO) Do not seek out data published online from a data breach. Malicious actors often embed malware, such as banking Trojans, onto websites that host breached data.
- (U//FOUO) In the event of a suspected malware infection, isolate infected computers immediately by disconnecting the network cable.
- (U//FOUO) Maintain operational security when using social networking websites.

(U//FOUO) Report incidents to your organization's data security/IT personnel.

(U//FOUO) For any questions or concerns you may have regarding the data breach, please contact info@sacrtac.org.

(U) Warning: This document is **Unclassified//For Official Use Only (U//FOUO)**. It contains sensitive information that cannot be released to the public or other personnel outside of the public safety community. To report suspicious activity to the CCIC, visit www.sacrtac.org.

UNCLASSIFIED//FOR OFFICIAL USE ONLY